Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

Michael F. Altschul
Senior Vice President, General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

Brian M. Josef
Assistant Vice President, Regulatory Affairs

CTIA-The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

July 18, 2013

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

In the Matter of	)	
	)	
Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities	)	GN Docket No. 13-111

COMMENTS OF CTIA – THE WIRELESS ASSOCIATION®

I. INTRODUCTION AND SUMMARY

CTIA – The Wireless Association® ("CTIA")[1] respectfully submits these comments in response to the Federal Communications Commission ("FCC" or "Commission") Notice of Proposed Rulemaking seeking to "remove barriers to the deployment and viability of existing and future technologies used to combat contraband wireless devices."[2]

CTIA supports the Commission's proposals to streamline its regulatory processes to speed the timeline for authorizing spectrum leases and Special Temporary Authority ("STA"). CTIA has concerns, however, with the proposal to require wireless providers to terminate service, if technically feasible, to wireless devices identified by cell detection systems as contraband, as detailed below.

The wireless industry has worked diligently with correctional institutions to put an end to the use of contraband wireless devices in prisons. Wireless providers have a strong record of cooperating with managed access system providers and correctional facilities to establish

[1] CTIA – The Wireless Association® is the international organization of the wireless communications industry for both wireless carriers and manufacturers. Membership in the organization includes Commercial Mobile Radio Service providers and manufacturers, including cellular, Advanced Wireless Service, 700 MHz, broadband PCS, and ESMR, as well as providers and manufacturers of wireless data services and products.

[2] *Promoting Technological Solutions to Combat Contraband Wireless Device Use in Correctional Facilities*, Notice of Proposed Rulemaking, FCC 13-58 (2013) ("NPRM").

spectrum manage lease arrangements in the numerous deployments and trials in states such as California, Maryland, Mississippi, South Carolina, and Texas.[3] CTIA submits, however, that more can be done to ensure the prompt deployment of managed access, and therefore supports the Commission's proposals to simplify its regulatory processes in this context.

The Commission also has proposed a requirement that wireless providers terminate service, if technically feasible, to a contraband wireless device when notified by an authorized correctional facility that has discovered the device through use of a cell detection system.[4] As CTIA has indicated in the past, detection systems have many advantages. However, CTIA is concerned that the CellAntenna proposal at issue in this proceeding raises many complex questions that have not been fully articulated by the Commission in the NPRM. In light of these complexities, CTIA cannot endorse the CellAntenna proposal at this time, and emphasizes that if the Commission nevertheless proceeds with this regime, it must adopt clear, standardized requirements that apply to all cell detection systems.

CTIA commends the Commission's strong stance in the NPRM against the unauthorized use of jamming systems to combat contraband wireless devices in prisons, as well as in other contexts.[5] CTIA strongly opposes the use of contraband cell phones in prisons and applauds the Commission's efforts to promote technologies that will combat this problem with minimal impact to legitimate uses.

---

3 *Id*. at ¶ 15.

4 *Id*. at ¶ 3.

5 NPRM at ¶¶ 18-19.

II. THE WIRELESS INDUSTRY HAS BEEN ON THE LEADING EDGE IN HELPING CORRECTIONAL ADMINISTRATORS COMBAT CONTRABAND WIRELESS DEVICE USE IN PRISONS.

CTIA is proud to report that its members have been on the leading edge of efforts to deploy managed access systems that help curb the use of contraband wireless devices in correctional facilities. These efforts, which were documented by the Commission in the NPRM, already have proven highly effective in addressing the contraband phone problem. The Commission is correct that the existing regulatory regime for establishing managed access systems could be reformed to enable a more efficient deployment. While CTIA is generally supportive of the Commission's proposals, in these comments it offers feedback on some specific elements of the Commission's proposed regime.

Managed access systems "are micro-cellular, private networks that analyze transmissions to and from wireless devices to determine whether the device is authorized or unauthorized for purposes of accessing public carrier networks."[6] There are a variety of managed access and detection systems that have proven highly effective in combating the use of contraband wireless devices in prisons, without the devastating effects associated with jammers. In just its first month of operation, the managed access system at the Mississippi State Penitentiary blocked 325,000 call and message attempts.[7] While the contraband device problem is not under the direct purview of wireless carriers, the wireless industry has been happy to cooperate with system providers to deploy managed access solutions, and has been pleased with the success of these systems.

---

6 NPRM at ¶ 14.

7 *Id.* at ¶ 15.

As the Commission observes in the NPRM, there have been ongoing cooperative agreements between wireless carriers and providers of managed access solutions to deploy systems that combat the use of contraband wireless devices in correctional facilities.[8] The Commission notes that this approach requires the negotiation of individual lease agreements between managed access providers and each wireless carrier licensed to provide service where the correctional facility is located. The existing regime, while producing positive results, is time-consuming, complex, and could delay the deployment of managed access systems. This could have the unintended consequence of discouraging the use of managed access systems.

The Commission has proposed several reforms to facilitate a streamlined application process for spectrum leases entered into "exclusively to combat the use of unauthorized wireless devices in correctional facilities."[9] CTIA agrees that these proposed rule and procedural changes are consistent with the Commission's intent to immediately approve leases that presumptively do not raise public interest concerns.[10] These changes include: (1) immediately processing managed access lease applications even where the lease would create a geographic overlap, (2) eliminating certifications related to the Commission's designated entity rules, and (3) modifying Form 608 such that applicants may easily identify that the lease application is exclusively for a managed access system in a correctional facility.[11] CTIA supports the Commission's proposed streamlining processes, and believes that the Commission's proposals are targeted, narrowly

---

8 *Id.* at ¶ 26.

9 *Id.* at ¶ 36.

10 *Id.*

11 *Id.* at ¶¶ 39-42.

focused, and will enable a more efficient deployment of managed access systems – a result plainly in the public interest.

While CTIA is generally supportive of the Commission's proposals, it offers comment on some specific issues raised by the Commission's proposed regime. First, the Commission has sought comment on whether it should apply its 911 and E911 rules to managed access services that provide access to 911 and E911. As the Commission notes, this is feasible as a technical matter.[12] CTIA takes no position on what action the Commission takes with respect to 911/E911 responsibilities of managed access systems. Since wireless providers have no ability to manage 911/E911 services when managed access solutions are used within correctional facilities, the Commission must make clear that wireless carriers should not be liable in the event that a call to 911 is blocked, or E911 data is degraded, by a managed access system.

Second, the Commission has proposed to streamline the process for a managed access provider to obtain STAs to operate a managed access system in a correctional facility. CTIA supports these proposals, so long as the existing requirement to obtain and demonstrate carrier consent continues to apply. The Commission notes that "[u]nder this process, applicants would still be required to meet all of the existing requirements to be granted STA."[13] While this presumably means that the carrier consent requirement would continue under the Commission's streamlined process, CTIA asks the Commission to make this requirement explicit in the rules it ultimately adopts.

---

12 *Id.* at ¶ 46.

13 *Id.* at ¶¶ 50-51.

III. THE COMMISSION'S PROPOSAL REGARDING DETECTION SYSTEMS RAISES COMPLEX ISSUES FOR WIRELESS CARRIERS.

Consistent with a petition by CellAntenna, the Commission has proposed to require CMRS licensees to terminate service to contraband wireless devices within correctional facilities pursuant to a "qualifying request from an authorized party."[14] This request would result from the use of a cell detection system to locate an unauthorized wireless device within the correctional facility. As the Commission explained in the NPRM, a cell detection system is very different than a managed access system. Detection systems are used to detect contraband devices within a correctional facility by locating, tracking, and identifying radio signals originating from a device. Prison administrators and correctional officers can then locate and confiscate unauthorized wireless devices within the prison. As CTIA has previously noted, cell detection systems "can provide correctional authorities and law enforcement with call records, address information, and even photographs that can assist in disciplinary actions and criminal prosecutions."[15] Several manufacturers have developed cell detection technologies and, in the past, the detecting and monitoring of contraband prison cell phones enabled authorities to combat criminal activity.[16]

CTIA has supported cell detection systems as a means of combating the use of contraband cell phones in prison facilities. However, CTIA is concerned that the CellAntenna

---

[14] NPRM at Appendix A, ¶ 8.

[15] Testimony of Steve Largent, President and CEO, CTIA – The Wireless Association® before the Senate Committee on Commerce, Science, and Transportation, Hearing on Contraband Cell Phones in Correctional Facilities: Public Safety Impact and the Potential Implications of Jamming, at 3 (July 15, 2009) ("Largent 2009 Senate Testimony, *available at* http://files.ctia.org/pdf/Testimony_CTIA_Largent_Contraband_Cell_Phones_7_15_09.pdf.

[16] Justin Fenton, *Indictments reveal prison crime world: Officers, inmates charged in drugs, extortion,* The Baltimore Sun (Apr. 17, 2009), *available at* http://articles.baltimoresun.com/2009-04-17/news/0904170011_1_corrections-staff-cell-staff-members.

proposal implicates many complex issues that have not been fully considered by the Commission in the NPRM. If the Commission does proceed along the route proposed by CellAntenna, at a minimum the Commission will need clear, standardized requirements that apply to all solutions.

A. The NPRM Has Not Fully Explored the Complex Questions Raised by the CellAntenna Proposal.

CTIA has previously voiced its support for the use of cell detection systems, noting the unique advantages of this technology.[17] CTIA takes this opportunity, however, to highlight some of the challenging questions that must be addressed and carefully resolved as the Commission contemplates CellAntenna's proposed regime.

As an initial matter, the Commission "note[s] the nexus" between CellAntenna's proposal and the wireless industry's recent voluntary commitment to take steps to deter smartphone theft.[18] However, the voluntary steps undertaken by carriers in this context are all premised on interactions between wireless carriers and their own customers and, thus, involve first-hand interactions within carriers' control. In the instant context, carriers would be interacting with non-subscribers making representations to carriers regarding subscriber devices, and would have less control than in the stolen phone database environment. The Commission must, therefore, consider its proposed rule against this backdrop and not assume the same level of carrier control that is present when dealing with the problem of stolen phones.

For CellAntenna's proposed framework to be effective, it is critical that wireless carriers receive complete and accurate information about the device to be shut off. CellAntenna has submitted that its systems can identify specific information about the device, including the

---

17 Comments of CTIA – The Wireless Association®, NTIA Docket No. 100504212-0212-01, at 13-17 (June 11, 2010) ("CTIA NTIA NOI Comments").

18 NPRM at ¶ 57.

service provider, electronic serial number, mobile identification number ("MIN"), international mobile equipment identifier ("IMEI"), or international mobile subscriber identity.[19] It is unclear from the NPRM who, if anyone, would certify the accuracy of the detection systems and attendant devices to increase the likelihood that information gathered by the prison is correct.[20] Carriers will require assurance that the information they receive is correct so that they do not inadvertently shut down wireless service to a bystander subscriber using a non-contraband device. The Commission would be best-positioned to provide such certification and should perform this role. Indeed, two important steps must be taken. First, even passive cell detection systems have the potential to produce emissions, and for this reason this equipment needs to be certified under Part 2 of the FCC's rules.[21] Second, there needs to be a process by which the Commission validates that a cell detection system is operating properly and capturing accurate, necessary information regarding potentially unauthorized phones. However, the NPRM does not address a certification or validation processes that need to be adopted. CTIA urges the Commission to develop Part 2 rules to govern the certification process. The Commission also should work with cell detection system providers to create a validation process (in addition to the certification process) that will verify that a cell detection system is properly functioning and

---

19 *See Amendment of Section 20.5 of the Commission's Rules, 47 C.F.R. § 20.5, to Categorically Exclude Service to Wireless Devices Located on Local, State, or Federal Correctional Facility Premises*, Petition for Rulemaking, PRM11WT, at 7 (filed Sept. 2, 2011) (CellAntenna 2011 Petition); NPRM at ¶ 62.

20 For example, many correctional institutions, especially minimum security "camps," may permit generally unsupervised visits on their grounds, thereby increasing the risk of the institution detecting a visitor's phone and instructing the carrier to disable a device that is not contraband.

21 *See* 47 C.F.R. §15.101 (defining unintentional radiators that should govern cell detection receivers) and 47 C.F.R. §2.801(b), §2.803 (requiring such unintentional radiators to be authorized prior to marketing/sale).

providing accurate and complete data that a wireless provider could rely upon prior to terminating service to a wireless device.

Next, the rule suggested by the Commission would expose wireless carriers to the significant risk of liability in the event that an authorized user's phone is inadvertently shut off, whether because the information supplied to the carrier contained a typographical error or any other reason. While CellAntenna has proposed a rule to "hold harmless" CMRS providers from violation of a law or regulation when the provider terminates service to a device while acting in good faith, the Commission's proposed rule includes no such provision.[22] Indeed, there is no rule that the Commission could adopt that would immunize a wireless provider from legal action – including tort action – at the federal or state level.

Further, it is unclear how the Commission's proposed rule, if adopted, would impact existing 911 call requirements. The Commission's "all calls" rule requires CMRS providers to forward all wireless 911 calls to Public Safety Answering Points.[23] It is unclear from the NPRM whether devices that are shut down pursuant to the CellAntenna proposed framework would remain subject to the "all calls" rule, and whether carriers would be required to connect calls from affected devices to 911. If carriers would be exempt from the "all calls" rule in this context, the Commission should make that clear. However, any regulatory framework that creates ambiguity with regard to wireless regulations, particularly in the context of emergency communications, places wireless carriers at great risk.

Finally, compliance with the proposed rule would be very burdensome for wireless carriers, impacting billing and customer service procedures. Carriers would need to explore and

---

22 NPRM at Appendix A, ¶ 8.

23 47 C.F.R. § 20.18(b).

adopt new internal procedures for ensuring compliance with the new requirements, and would need to extensively train customer service representatives. Not only will the carriers need to train the personnel directly responsible for terminating service, but carriers will also need to train their customer service representatives and address impacts on billing from termination.

Without resolution of unanswered questions such as those discussed above, CTIA cannot endorse the CellAntenna proposal at this time. If the Commission nevertheless proceeds with this approach, at a minimum it will need clear, standardized requirements that apply to all cell detection systems with equal force. CTIA discusses these requirements below.

B. Any Framework Adopted Must Contain Clear, Standardized Requirements.

Clarity and certainty will be vital if the Commission is to adopt service termination requirements in connection with unauthorized wireless devices in correctional facilities. First, if carriers will be required to terminate service under these circumstances, the bar for compelling carriers to act must be strictly limited and clear. The NPRM envisions that a designated prison employee would be responsible for notifying carriers of devices whose service must be terminated. The Commission's proposed rule simply says that a "qualifying authority" would identify contraband devices to CMRS providers, without defining the term.[24] Many correctional institutions and detention centers are privately owned and operated. Wireless providers should not be required to respond to requests by non-sworn law enforcement officials. CTIA submits that the procedures to trigger this requirement should be made clear and unambiguous, and that it should be clear which entity is responsible for notifying the carrier.[25] This will benefit departments of corrections as well as wireless providers.

---

[24] NPRM at Appendix A, ¶ 8.

[25] For example, CTIA has previously highlighted situations where prison officials and law enforcement have worked together and determined to leave detected devices in place and

CTIA proposes two potential Commission rules that could help promote this clarity. First, CTIA notes that the proposed rules contain a definition for a managed access system, but not for a cell detection system. CTIA submits that both technologies should be formally defined. CTIA does not take a position on the rule section where the Commission would define "cell detection system," but proposes the following definition:

> "*Cell detection system.* A cell detection system is a system that: (1) uses passive, receive-only technology exclusively to locate, track, and identify unauthorized wireless devices within the boundaries of a correctional facility; (2) has been certified by the Commission through its equipment certification process; and (3) has been validated by the Commission as accurately identifying and locating unauthorized wireless devices. Any system that contains a transmitting element but otherwise satisfies this definition is considered a managed access system as defined in section 1.9003 of the Commission's rules."

Adoption of this definition would serve a number of important objectives. First, it would make clear which technologies would implicate any termination requirement adopted by the Commission (see proposed revisions to Sec. 20.21 below). Second, it would enable and codify the necessary certification steps outlined above. Third, it would ensure that all solutions containing a transmitting element operate only with carrier consent. CTIA notes that at the outset, the Commission has stated that "[d]etection systems use passive, receive-only technology and do not transmit radio signals."[26] However, there are cell detection systems, such as CellAntenna's Guardian solution, that do transmit on carrier frequencies.[27] CTIA stresses that at

---

monitor them in accordance with wiretap statutes. CTIA NTIA NOI Comments at 13-14. In this context, there would likely be multiple authorities involved in the identification and documenting of a contraband phone, and officials may even change their mind regarding the chosen disposition of a contraband phone. In this and similar situations, clarity for wireless carriers regarding the action to be taken is vital.

[26] NPRM at ¶ 16.

[27] *See* http://www.cjam.com/index.php?id=cjamguardian. CellAntenna highlighted the Guardian system in particular when it filed its Petition at the FCC. Press Release, CellAntenna, "CellAntenna Files Petition at the FCC to Get Illegal Cell Phones Found in Prisons Turned off

no time may a detection system transmit on carrier frequencies without a lease or STA. For this reason, CTIA submits that such systems are more properly classified as managed access systems, and has crafted its proposed definition of "cell detection system" accordingly.

Second, CTIA proposes that the FCC revise its proposed service termination rule as follows:

> "§ 20.21 Service termination upon notice of an unauthorized user.
>
> "CMRS providers are required to terminate service to any device identified by a cell detection system (as defined in [rule section]) ~~qualifying authority as~~ and determined to be unauthorized within the confines of a correctional facility, as ordered by a court of relevant jurisdiction."

As noted above, CTIA submits that the Commission's use of "qualifying authority" in the existing proposed rule is too vague, and could create uncertainty for carriers with respect to which state official must issue the termination request. By requiring that the notice come from a court of relevant jurisdiction, the Commission would ensure a high standard for such requests and provide much-needed clarity to CMRS providers.

IV. CONCLUSION

CTIA is proud of the role its wireless industry members have played in assisting correctional administrators in their fight against the use of unauthorized, contraband wireless devices in correctional facilities. CTIA supports the Commission's efforts to streamline the cooperative efforts of wireless carriers and managed access providers. While CTIA also believes that cell detection technology is a valuable tool in this effort, the Commission's service

---

by Cell Phone Carriers" (Sept. 6, 2011), *available at* http://www.businesswire.com/news/home/20110906005585/en/CellAntenna-Files-Petition-FCC-Illegal-Cell-Phones.

termination proposal requires further evaluation. To the extent the Commission does adopt rules, these rules must promote clarity and certainty for wireless carriers.

Respectfully submitted,

By: */s/ Brian M. Josef*

Brian M. Josef
Assistant Vice President, Regulatory Affairs

Michael F. Altschul
Senior Vice President and General Counsel

Scott K. Bergmann
Vice President, Regulatory Affairs

CTIA-The Wireless Association®
1400 Sixteenth Street, NW
Suite 600
Washington, DC 20036
(202) 785-0081

Submitted: July 18, 2013